資料７

NISC National Information Security Center

「重要インフラの情報セキュリティ対策に係る行動計画」の見直し
（事務局案説明資料）

個別論点（第2回）

2008年 7月18日
内閣官房 情報セキュリティセンター
（NISC）

今回の検討範囲（1）

○ 今回と次回で「4-2 行動計画の基本的枠組みに関する事項」の積み残り事項に加え、「4-3 安全基準等の整備」「4-4 情報共有体制の強化」「4-5 相互依存性解析・分野横断的演習」を検討し、とりうる方向性を確認したい
○ なお、「4-1 本委員会の議論等を通じて認識された課題」については、全体にかかる論点であるため、今回のみならず、次回以降も随時議論し、最終的に基調となる方向性を設定したい

検討テーマ（論点整理における項目）	現行動計画における項目	該当ページ
4-1 本委員会での議論等を通じて認識された課題	（全体）	p3
4-2 行動計画の基本的枠組みに関する事項		
①対策の目的（目標）、視点	1 目的と範囲	p4
②「重要インフラ分野」の分類、位置づけ	2 重要インフラの定義と対象 別紙1 各重要インフラ分野において対象となる重要システム等	p7
③枠組みの柔軟化		p9
④「重要インフラ事業者等」「重要システム」		p15
⑤IT障害への脅威の例示	2(2)ア IT障害への脅威の例示	p16
⑥他の取組みとの関係の整理	1 目的と範囲	p18
⑦評価の手法	8(1) 進捗状況の評価・検証	p19
4-3 安全基準等の整備	（3 重要インフラにおける情報セキュリティ確保に係る「安全基準等」）	
①「指針」の位置づけ、記載内容の具体性のレベル	3(1) 位置づけ 指針　Ⅰ目的及び位置づけ	p20
②事業者等のPDCAサイクルとの整合性	3(1) 位置づけ 指針　Ⅲフォローアップ	p24
③事業継続計画との関係	指針　Ⅱ「安全基準等」で規定が望まれる項目	p27
④リスク開示の在り方		p29

※今回の議論にて積み残った内容は、引き続き次回以降にて議論を継続

今回の検討範囲（2）

検討テーマ（論点整理における項目）	現行動計画における項目	該当ページ
4-4 情報共有体制の強化	（4 情報共有体制の強化）	
①情報共有の目的等について	（頭書き）	p30
②NISCの役割について	4(1)　官民の情報提供・連絡	p32
③「情報共有」の障害除去	―	p33
④CEPTOARについて	4(2)　情報共有・分析機能	p35
⑤その他	―	p36
4-5 相互依存性解析・分野横断的演習		
①相互依存性解析の継続について	5 相互依存性解析	p37
②分野横断的演習の継続について	6 分野横断的な演習	p38
③「事案対処」の観点からの課題検証について	―	p39
④その他	―	p40
4-6 その他		
①NISCの果たすべき役割		
②国際的取組みとの整合性について		
③各主体において取り組むべき事項と横断的施策について		
④行動計画の推進体制について		
自由討議		

※今回の議論にて積み残った内容は、引き続き次回以降にて議論を継続

4-1 本委員会の議論等を通じて認識された課題

○ 行動計画の見直しのとりまとめに際して、最終的に以下の点について採るべき方向性を示せるよう、個別の論点の検討を行う

○各重要インフラ分野において、ITへの依存度（ITの機能不全とサービス低下の距離感）、ITの観点での他分野との相互依存性などは様々である。それに応じた各分野における取組みにも多様性が存在する。

→ 全分野・全事業者に一律の対策を求め平均を底上げするか、個別の進んだ対策を伸ばすか

○情報セキュリティ対策を考える際には、経営（コスト配分・サービスの維持レベルなど）やコンプライアンス、内部統制の視点も踏まえるべき要素の一つである。

→ 対策の対象はITのみに限定するか、ITを含めた経営全体か

○重要インフラ事業者等の立場から見ると、「個々の利用者（顧客）」へのサービス提供と「公益」の観点から求められる対応の2つの側面があり、両者は必ずしも常に一致するものではない。

→ 事業者等の自発的な取組みに重点をおくか、社会的要請に基づく取組みに重点をおくか

○IT障害から重要インフラを防護する観点からは、障害の未然防止だけでなく、障害発生時に影響を最小限に抑えるための対応（早期対応、応急対応など）も重要である。

→ 緊急時対応を国や他事業者と連携して行うのか、事業者独自の取組みに任せるのか

○個々の重要インフラ事業者等による情報セキュリティ対策については向上が進んでいるものと考えられるが、障害（リスク）の発生時の情報や、「経験」から得られる知見の共有については、今後の一層の取組みについて、検討を進めるべきである。

→ どのような知見を共有対象とすべきか
IT障害に至らない事象（ヒヤリ・ハット等）も重視すべきではないか

事務局案（4-2 行動計画の基本的枠組みに関する事項①）

①対策の目的（目標）、視点　【重要整理事項】

○「重要インフラにおけるIT障害発生ゼロ」よりも適切な目標はあるか

- 第1次情報セキュリティ基本計画において、2009年度初めの目標として、以下が挙げられている
  - 政府機関：すべての政府機関において、政府機関統一基準が求める水準の対策を実施
  - 重要インフラ：重要インフラにおけるIT障害の発生を限りなくゼロに
  - 企業：企業における情報セキュリティ対策の実施状況を世界トップクラスの水準に
  - 個人：「IT利用に不安を感じる」とする個人を限りなくゼロに
- 現行動計画において以下の目的が挙げられている
  - 重要インフラ事業者等のサービスの維持
  - IT障害発生時の迅速な復旧等の確保
- 【専門委員会での議論より得られた方向性】
  - 象徴的な目標として、「IT障害の発生を限りなくゼロに」は適切
  - 一方で、評価と連動した定量的で測定可能な目標についても検討が必要
    - 何をいつまでに達成したいか明確にする
    - 合理的な目標水準を定義する（例：「国民生活や社会経済活動に重大な影響」を及ぼすIT障害発生ゼロを目指す　等）
- 【基本計画検討委員会（「次期情報セキュリティ基本計画に向けた第１次提言」）より】
  - 「事故前提社会」への対応力強化に向けて、発生した問題に対して許容可能な水準を設定していくことが提言されている

【事務局案】
- 究極的な目標である「基本理念」と、合理的な達成水準を具体化した「政策目標」を分けて議論
- 「基本理念」は、「IT障害の発生を限りなくゼロに」又はそれに類するものを策定する
- 「政策目標」は、維持すべきサービスレベルを分野毎に定める
  - 「③枠組みの柔軟化」でのサービスの検討を踏まえて検討する
  - 各分野の特性に応じた自発的な取組みとして努力目標を定める
  - IT障害に至る以前の（至らないための）対応についても目標に加えてはどうか

事務局案（4-2 行動計画の基本的枠組みに関する事項①）

○「未然防止」「拡大防止」「再発防止」のバランスをどう考えるか、いずれかに重点をおくべきか

- 現行動計画において上記3つの観点が書かれているが、次の一手を進めるためには行動計画にて予め重点をおくべき点を明らかにすべきという考え方がある
  - 一方、情報提供等を受けて対策する側が判断すべきこととして、特に重点を置くべきではないという考え方もある
- 以下2つの対応が考えられる
  - 案1：全てに取り組む
  - 案2：いずれかに重点をおく
    - 案2－1：4つの柱の施策毎に必要性等を踏まえて判断する
    - 案2－2：行動計画全体にかかるテーマを定める
- 【専門委員会での議論より得られた方向性】
  - （特になし：後日検討）

【事務局案】
・個別施策における具体的な取組みの検討を踏まえて議論することが望ましいため、後日検討（後述する「⑤IT障害への脅威の例示」及び「4-4 情報共有の体制の強化」での取組み内容の検討を踏まえて策定）

事務局案（4-2 行動計画の基本的枠組みに関する事項①）

○個人情報保護の観点をどう位置づけるべきか

- 一般に個人情報保護法において「個人情報保護取扱事業者」には、個人情報の適正な取扱いの確保が求められている
- 現行動計画は、「重要インフラ事業者等の自主的な対策について示す」こととしている
- 【専門委員会での議論より得られた方向性】
  - （特になし：事務局案のとおり）

【事務局案】
・個人情報保護法が制定されていることを踏まえると、法令遵守の観点から当然対応が必要なものであり、重要インフラ事業者向けとして特に行動計画において求めるべきことは現時点では少ないのではないか

現行動計画「1 目的と範囲」より（抜粋）
・（IT障害）から国民生活や社会経済活動に重大な影響を及ぼさないよう重要インフラを防護し、重要インフラ事業者等の事業継続への取組みを強化するための取ることが望ましい**重要インフラ事業者等の自主的な対策**について示す

事務局案（4-2 行動計画の基本的枠組みに関する事項②）

②「重要インフラ分野」の分類、位置づけ　【重要整理事項】

○現在の10分野の分類や位置づけは適切か、実態に即し見直し（分割・追加等）の必要はないか

- 諸外国における重要インフラの分類（次ページ）等を参考に、見直し（分割・追加等）が望まれる分野はないか
  例） クレジットカード会社（消費者信用）、ITベンダー（情報技術） 等
- 現在の10分野とは別に、協力を求めるべき業界があれば、何らかの形で位置づけることも考えられる
- 現在の10分野についても、ITへの依存度等に応じて分類や位置づけを何段階かに整理することも考えられる
- 重要インフラの定義そのものについても、必要に応じて見直しを検討することが考えられる
- 【専門委員会での議論より得られた方向性】
  - （特になし：事務局案のとおり）

【事務局案】
・ 新たな分野を加えるのではなく、現在の10分野を踏襲しつつより内容を充実させてはどうか

現行動計画「2 重要インフラの定義と対象」より（抜粋）
・ 重要インフラとは、「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもの」と定義
・ 当面の対象分野は、「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」の10分野

＜参考＞諸外国における重要インフラの分類

国名	我が国10分野との対応関係（各国における名称）　※各分野の範囲は必ずしも一致しない										
	情報通信	金融	航空	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	その他
オーストラリア	通信	銀行・金融	交通		エネルギー		ー	健康	水道	ー	食料供給、緊急時対応、名所と公の集会
カナダ	通信・情報技術	金融	交通		エネルギー・設備		政府	公衆衛生	水道	ー	食料、製造、安全保障
フランス	通信	銀行・金融	交通システム		エネルギー・電力、原子力発電所		ー	公衆衛生	水道供給	ー	化学・バイオ産業、公安秩序
ドイツ	情報通信・情報技術	金融・保険	交通・運輸		エネルギー		行政・司法	ー	ー	ー	サービス、危険物、その他
韓国	情報通信、メディアサービス	金融サービス	交通		ガス・エネルギー		電子政府・国家行政	ー	ー	ー	緊急時対応、国家防衛
シンガポール	情報・通信	銀行・金融	陸上・航空・海上輸送		エネルギー		ー	健康	水道	輸送	極めて公的な場所、注目を集めるイベント
ロシア	情報・通信システム、マスメディア	クレジット・金融	交通		エネルギー		連邦政府関連情報	ー	ー	ー	国内産業、軍事
スウェーデン	情報通信システム、インターネット	金融システム	航空管制	ー	ー	ー	ー	ー	水道・輸送・産業における監視・制御		国家指令システム
英国	通信	金融	交通		エネルギー		政府	衛生	水道	ー	食料、緊急時対応
米国 ※KR（Key Resources：重要資産）含む	通信	銀行・金融	交通		エネルギー		政府施設	公共衛生・医療	水道	郵便・宅配	農業・食料、化学、商業施設、ダム、防衛産業基盤、緊急時対応、情報技術、国家象徴・モニュメント、核物質取扱・廃棄設備

※重要情報インフラ防護（CIIP）の観点に限らない点注意

（出典）CIIPハンドブック2006　http://cipp.gmu.edu/archive/5_IntlCIIPHandbook_2006_Vol_I_Switz.pdf　及び各国ホームページ

事務局案（4-2 行動計画の基本的枠組みに関する事項③）

③枠組みの柔軟化

【重要整理事項】

○ **ITへの依存度、インターネットとの接続（直接・間接）、維持すべきサービスレベル、社会や利用者への影響の度合い、分野間の依存関係、事業規模等を踏まえ、対策の優先度を分野や事業者等単位などで柔軟に考えるべきではないか**

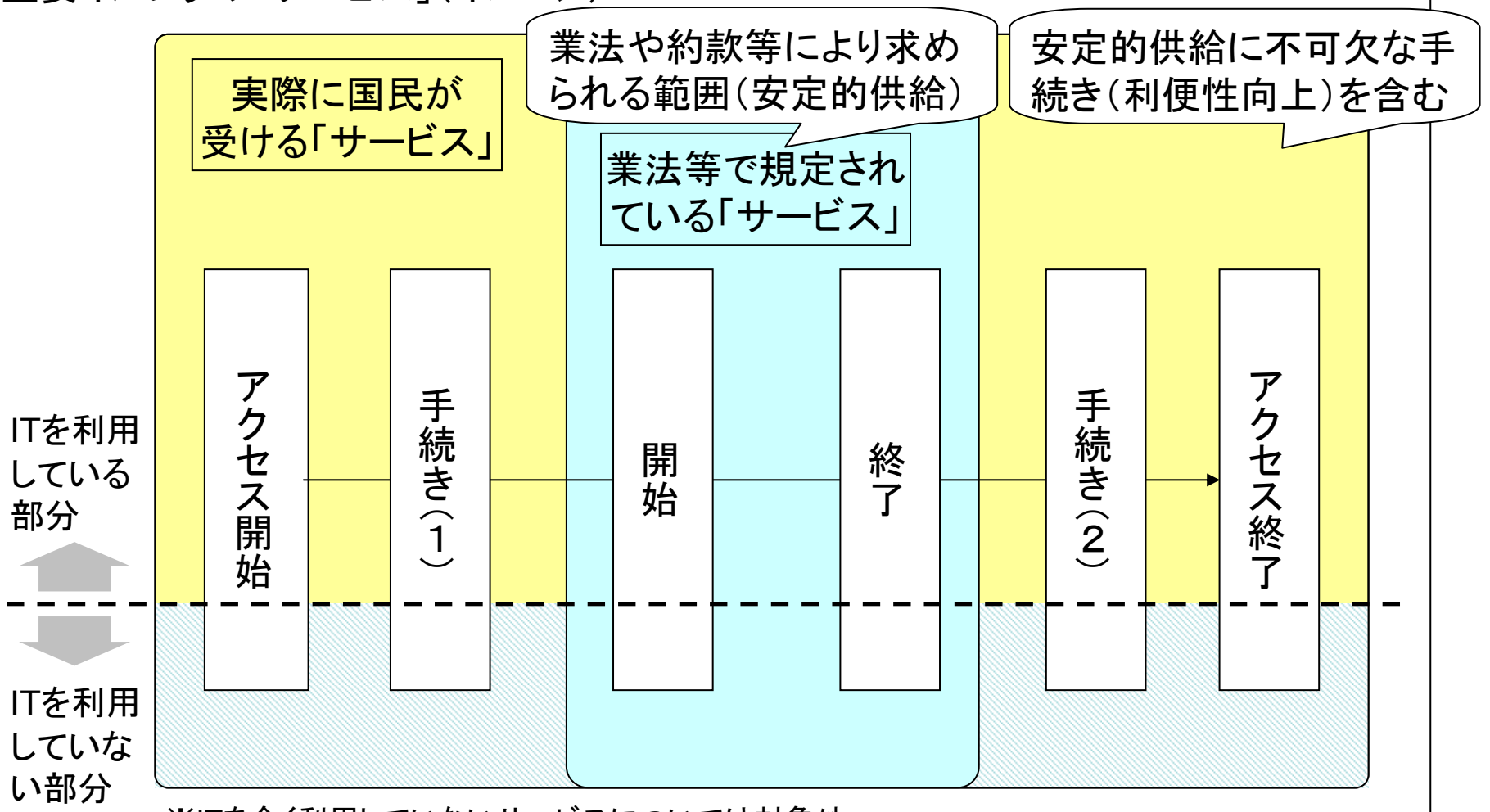
- 現行動計画では「重要インフラ」の定義はあるが、対象とするサービスについての利用側と提供側のギャップが存在している
- 多くの論点についての方向性を整理する軸として、まずは行動計画の対象とする重要インフラの「サービス」を定義し、その範囲と水準を洗い出す必要があるのではないか
- 【専門委員会での議論より得られた方向性】
  - 現行動計画の重要システムの例示から各分野のサービスは想定されているとともに、既に相互依存性解析でサービスを定義している
  - 「他で代替することが著しく困難なサービス」に限定して議論するべき
  - 重要インフラ事業者である以上、規制対象となる事業以外にも、社会の期待に応えて取組むべき
  - 国民（利用側）視点から見た部分が入らないのであれば、その理由を明確にする必要がある
  - 事業者等のサービスの中で、どこまでが入るのかという切り口を確定する必要がある

【事務局案】
・サービスの ITへの依存は、時代とともに変化することを踏まえ、現時点でのITへの依存度に拘らず、一旦広くサービスを洗い出してはどうか
・従来より事業者等（提供側）が対策を取っている業法等で規定されている「サービス」とそのサービスレベルに限らず、現行動計画の「重要インフラ」の定義の範囲で、実際に国民（利用側）が受ける「サービス」を対象としてはどうか
・「サービスの具体化（たたき台）」を元に、具体的にどの範囲のサービスを対象とし、「政策目標」としてサービスレベルの努力目標をどこにおくかを委員の協力を得つつ検討してはどうか

現行動計画「1 目的と範囲」より（抜粋）
・ 重要インフラ事業者等のサービスの維持及びIT障害発生時の迅速な復旧等の確保を図るため、内閣官房を中心とした政府及び各重要インフラ分野において実施することが望ましい施策を既存の法令、防災計画等の枠組み等との整合を図りつつ具体化

事務局案（4-2 行動計画の基本的枠組みに関する事項③）

重要インフラの「サービス」（イメージ）



※ITを全く利用していないサービスについては対象外

※現行動計画の「重要インフラ」の定義より、以下の範囲でサービスを具体化

- 他に代替することが著しく困難なサービスを提供する事業が形成する国民生活や社会生活の基盤
- その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じる

サービスの具体化（たたき台）：業法や約款等により求められる範囲

分野		業法等で規定されているサービス	根拠法（条）	その他
情報通信		・電気通信役務（電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供すること）を他人の需要に応ずるために提供	電気通信事業法（2条）	
		・公衆によつて直接受信されることを目的とする無線通信の送信	放送法（2条）	
金融	銀行 生命保険・損害保険 証券会社 証券取引所	・預金又は定期積金等の受入れ、資金の貸付け又は手形の割引、為替取引、その他銀行業に付随する業務 ・人の生死に関し一定額の保険金を支払うことを約し保険料を収受する保険、一定の偶然の事故によって生ずることのある損害をてん補することを約し保険料を収受する保険その他の保険の引受けを行う事業 ・金融商品取引業、金融商品仲介業、金融商品市場	銀行法（10,11,12,12-2条） 保険業法（2条） 金融商品取引法（1条）	
航空		・他人の需要に応じ、航空機を使用して有償で旅客又は貨物を運送する事業	航空法（2条）	
鉄道		・他人の需要に応じ、鉄道による旅客又は貨物の運送を行う事業	鉄道事業法（2条）	
電力		・一般電気事業（一般の需要に応じ電気を供給する事業） ・卸電気事業（一般電気事業者にその一般電気事業の用に供するための電気を供給する事業）	電気事業法（2条）	特定電気事業、特定規模電気事業
ガス		・一般ガス事業（一般の需要に応じ導管によりガスを供給する事業）	ガス事業法（2条）	簡易ガス事業、ガス導管事業、大口ガス事業
政府・行政サービス		・市民の命に関わるサービスや橋・道路等のインフラ整備に係るサービスの他、学校や障害者・高齢者への医療・福祉・介護・保健等の各種サービスが多数存在する	（業法なし：相互依存性解析報告書より転記）	
医療		・医療機関の開設及び管理	医療法（1条）	助産所の開設及び管理
水道		・一般の需要に応じて、水道により水を供給する事業（給水人口が100人以下のものを除く） ・水道により、水道事業者に対してその用水を供給する事業	水道法（3条）	専用水道
物流		・貨物利用運用事業（他人の需要に応じ、有償で、利用運送を行う事業） ・貨物自動車運送事業（他人（又は特定）の者の需要に応じ、有償で、自動車を使用して貨物を運送する事業） ・倉庫業（寄託を受けた物品の倉庫における保管を行う営業）	貨物利用運送事業法（2条） 貨物自動車運送事業法（2条） 倉庫業法（2条）	

サービスの具体化（たたき台）：安定的供給に不可欠な手続き（利便性向上）

分野	アクセス開始－手続き（1）に相当するサービス	手続き（2）－アクセス終了に相当するサービス	その他
情報通信	（イメージ） ・利用予約 ・利用申込 ・利用券購入 ・利用受付 ・利用入口通過	（イメージ） ・料金収納 ・料金精算 ・利用出口通過	（イメージ） ・サービス提供状況案内
金融：銀行 生命保険・損害保険 証券会社 証券取引所			
航空			
鉄道			
電力			
ガス			
政府・行政サービス			
医療			
水道			
物流			

・現行動計画　別紙1「対象となる重要システム例」から類推されるサービスも含め広く洗い出す
・これらのサービスにおける、ITの活用の程度については、個々事業者等の経営判断によるものであり、本表にサービスを掲載することによって、必ずしも全事業者等が当該サービスにITを活用していることを意味していない

サービスの具体化（たたき台）：委員への依頼事項

○ 「サービスの具体化（たたき台）」はサービスを広く洗い出すための端緒とすべく、事務局において整理したもの
○ 今後の検討を進めるにあたって、各委員においてはサービスの洗い出しにご協力いただきたい

業法や約款等により求められる範囲 （P11）

【たたき台の考え方】
- 「業法等で規定されているサービス」を各事業法を参考に整理
- 必ずしも業法の正確な引用ではない
- 「その他」は、根拠法上にて記載はあるが、現行動計画　別紙１の「対象となる重要インフラ事業者等」に記載がないもの

【委員への依頼事項】
- **根拠法令等からサービスの定義が可能なものについて、一旦広くそのサービスを洗い出し、根拠法令等と併せてお知らせいただきたい**

安定的供給に不可欠な手続き（利便性向上） （P12）

【たたき台の考え方】
- 「利用申込」等、一連の手続きとして「業法で規定されるサービス」につながると考えられるものを整理
- 「その他」の欄には、一連の手続きではないが国民生活や経済活動への影響があると考えられるものを整理
- ITを使用しないものや、IT以外の代替手段があるものも含めて、一旦広く洗い出し

【委員への依頼事項】
- **IT利用の範囲が「業法や約款等により求められている範囲」の外側にも拡がりつつある現状をふまえた議論をするために、一旦広く考えてサービスを洗い出し、お知らせいただきたい**

＜参考＞今後の進め方（案）

- 各委員の意見を取りまとめて提示した後に、ITへの依存度・インターネットとの接続等を踏まえて防護対象にすることが適切かを検討（対象外とする場合は、その理由も整理）
- 防護対象とするサービスについて、「政策目標」としてサービスレベルの努力目標を設定し、行動計画に反映することを検討

事務局案（4-2 行動計画の基本的枠組みに関する事項③）

○「分野」単位よりも「事業者等」単位の方が進捗しやすい事項もあるのではないか

- 現行動計画は、「重要インフラ事業者等の自主的な対策について示す」こととしている
  - 分野単位で考えると、事業規模の小さい事業者等を含め、全事業者が対応しうる最低限の対策になりがちではないか
  - 分野内のいわゆるトップランナー的な事業者にて行われる取組みも含めるべきではないか
- 個別施策の中で検討するという考え方もある
- 【専門委員会での議論より得られた方向性】
  - 分野単位が基本であるので、事業者単位はオプションとして考えるのがよい
  - 「ITへの依存度等に応じて分類や位置づけを何段階かに整理」を行うことで、トップランナー的な事業者にて行われる取組みが浮き上がるのではないか

【事務局案】
・対策の優先度を分野や事業者等単位などで柔軟に考え、分野の一部の事業者等がとりうる対策事項についても、行動計画の取組みとして検討してはどうか
・「サービスの具体化（試案）」の検討及び各施策毎の次期行動計画における取組み内容の検討を踏まえて策定

事務局案（4-2 行動計画の基本的枠組みに関する事項④）

④「重要インフラ事業者等」「重要システム」　【重要整理事項】

○行動計画の別紙1に掲載されている「重要インフラ事業者等」や「重要システム」について、実態や利用者の観点に即した修正の必要はないか

- 一般企業としてではなく、重要インフラとして位置づける事業者の範囲をどこにおくか
  - 分野によって事業者を一部の範囲に限定してよい場合があるのではないか
  - 事業者のサービス停止・機能低下の影響が多方面に及ぶ場合、当該事業者が対象事業者に含まれているか
  - 例えば判断基準としては、市場占有率が一定以上ある場合や指定公共機関等として公共的な役割が求められている場合などが考えられないか
- 2007年度の指針の見直しでは、「安全基準等の適用対象とならないシステムも含めて、我が国の国民生活や社会経済活動に影響をおそれが生じる障害が発生」していることが明らかとなっている
  - 行動計画の対象範囲は、例示された重要システムに限定できないのではないか
    （例えば、バックオフィスのシステム障害がサービスへ影響する場合はないのか）
- 【専門委員会での議論より得られた方向性】
  - 行動計画別紙1の表を拡張して、「サービス」を記述すべき
  - 分野毎にサービスを議論してから、システムの議論を行うことにより、重要システムはサービスを支えているシステムであるという部分について明示的に示すことが重要
  - 既に相互依存性解析の成果として、分野毎の「サービス」についてのたたき台はできているので、議論の前提として提示してほしい

【事務局案】
・実態や利用者の観点に即した修正に加え、論点整理に対するこれまでの方向性を踏まえ、サービスの観点を切り口として、別紙1の項目立てを見直してはどうか

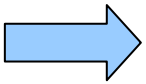
事務局案（4-2 行動計画の基本的枠組みに関する事項⑤）

⑤IT障害への脅威の例示

【重要整理事項】

○現在の脅威の例示は、実態に即して適切か

- 各事業者の取組みにおいて、脅威の例示は適切であったと評価できるか
  - 昨今の社会状況等を踏まえ、新たに加えるべき脅威はないか
    例） パンデミック（新型インフルエンザの世界的流行）
- 各事業者毎に脅威に対する対策が可能か、あるいは分野横断的な対応が必要になるか
- 【専門委員会での議論より得られた方向性】
  - （基本的な方向性は事務局案のとおり）



【事務局案】
・対応主体別に、個別の重要インフラ事業者等が中心となって対応する脅威と、社会全体で対応が望まれる脅威を峻別して、脅威の例示を新たに加えてはどうか
・サービスの停止の他分野への波及等、現行動計画での取組みにより新たな「他に与える脅威」が判明していることから、脅威の例示をくわえてはどうか
・現在の脅威の例示については、「自ら受ける脅威」として、表現の適正化等全体を見直ししてはどうか
・「対応主体に注目したIT障害への脅威の例示（たたき台）」を元に、具体的な脅威の例示を見直してはどうか

現行動計画「2 重要インフラの定義と対象」より（抜粋）
①サイバー攻撃によるIT障害への脅威
　不正侵入、データ改ざん・破壊、不正コマンド実行、ウィルス攻撃、サービス不能攻撃（DoS: Denial of Service）、情報漏えい、重要情報の搾取　等
②非意図的要因によるIT障害への脅威
　操作・設定ミス、プログラム上の欠陥（バグ）、メンテナンス不備、内部・外部監査機能の不備、外部委託、マネジメントの欠陥、内部不正　等
③災害によるIT障害への脅威
　地震、水害、落雷、火災等の災害による電力供給の途絶、通信の途絶、コンピュータ施設の損壊等、重要インフラ事業者等におけるITの機能不全

対応主体に注目したIT障害への脅威の例示（たたき台）

脅威の種類		IT障害への脅威の例示	
		社会全体で対応が望まれる脅威	個別の重要インフラ事業者等が中心となって対応する脅威
自ら受ける脅威	①サイバー攻撃をはじめとする意図的要因によるIT障害への脅威	・分野横断的に多発するサービス不能攻撃、不正侵入、重要情報の搾取　等	不正侵入、データ改ざん・破壊、不正コマンド実行、ウィルス攻撃、サービス不能攻撃（DoS: Denial of Service）、情報漏えい、重要情報の搾取、内部不正　等
	②非意図的要因によるIT障害への脅威	・大規模な操作・設定ミス、プログラム上の欠陥（バグ）、メンテナンス不備が予想される社会環境変化や制度改正（例：西暦2000年問題、暗号の危殆化、IPv6への移行）　等	操作・設定ミス、プログラム上の欠陥（バグ）、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥　等
	③災害や疾病によるIT障害への脅威	・大規模な地震、水害（例：首都圏直下地震、荒川の氾濫）による電力設備の損壊、通信設備の損壊、水道設備の損壊、コンピュータ施設の損壊　等 ・パンデミック（例：新型インフルエンザの大流行）によるオペレータの不足　等	地震、水害、落雷、火災等の災害による電力設備の損壊、通信設備の損壊、水道設備の損壊、コンピュータ施設の損壊　等
他に与える脅威	④他分野への波及によるIT障害への脅威	・大規模な電力供給の途絶、通信の途絶、水道供給の途絶（相互依存性解析の成果で判明しているもの）　等	電力供給の途絶、通信の途絶、水道供給の途絶（相互依存性解析の成果で判明しているもの）　等

※　下線部分は現行動計画からの追記部分

事務局案（4-2 行動計画の基本的枠組みに関する事項⑥）

⑥他の取組みとの関係の整理　【重要整理事項】

○情報共有や連携の部分で、防災担当機関や事案対処省庁、その他関係機関の取組みと競合する部分はあるか、補完しあえる部分はどこか

- 分野横断的演習において、「「事案対処」の観点からの課題検証について」として個別に論点があげられている
- 基本計画検討委員会においても、他の関係機関との連携について検討の予定がある
- 【専門委員会での議論より得られた方向性】
  - 現行動計画で基準と枠組みが整理された後、次期行動計画では具体的なオペレーションに焦点を置く段階になるため、事案対処省庁をきちんと枠組みの中に入れ、議論していくべき
  - 既に論点整理であげられた「重要インフラ事業者等の自主的な取組みが大原則であることを踏まえつつ、官民の役割・責任の適切な分担」を基本的スタンス・視点におきつつ検討する

→ 【事務局案】
・個別施策における具体的な取組みの検討や基本計画検討委員会での検討を踏まえて議論することが望ましい
・国民生活や社会経済活動の維持に向けた重要インフラ事業者等の事業継続の取組みに対して、具体的にどのような協力が可能であるかについて事案対処省庁からの提案を受けて検討

○個々の事業分野における業法との関係で競合する部分はあるか

- 他分野の事業継続のために、自分野の業法で規定される以上の対応を求められる場合があるのではないか

→ 【事務局案】
・個別施策における具体的な取組みの検討を踏まえて議論することが望ましいため、後日検討

事務局案（4-2 行動計画の基本的枠組みに関する事項⑦）

⑦評価の手法　【重要整理事項】

○目標、評価指標、対策の進捗度合いの把握方法等について、どう設定すべきか

- 現行動計画では、プロセス評価（目標に対する実施状況の把握）を中心に実施
  - 上記に加え、2007年度は補完調査（参考となるデータの補足、具体的事例の検証）を実施
- 現行動計画は、「重要インフラ事業者等の自主的な対策について示す」こととしている
- 行動計画の取組みの内容を固めることが先決であるという考え方もある
- 【専門委員会での議論より得られた方向性】
  - サービスの提供側でなく、利用側視点での指標が求められている
  - 世の中がどう変わるかのアウトカムを説明することが求められている
  - どのような記録を元に、どのように評価するのかを明らかにする必要がある

【事務局案】
・基本計画検討委員会より、情報セキュリティ基本計画の全体的な視点からのインプットが想定されているため、その内容を受けて後日検討
・ サービス毎の具体的な目標水準の検討、及び各施策毎の次期行動計画における取組み内容の検討を踏まえて策定

事務局案（4-3 安全基準等の整備①）

①指針の位置づけ、記載内容の具体性のレベル　【重要整理事項】

○「指針」に記載される事項について、「安全基準等」に盛り込む「べき」事項と盛り込むことが「望ましい」事項に仕分けをし、その位置づけを明確にすべきではないか

- 現行の「指針」では、「何らかの対処がなされていることが望ましい項目を列記」している
- 現行の「指針」を踏まえ、各分野の「安全基準等」が以下のとおり整備されている
  - 大半の「安全基準等」は、「強制基準」ではなく「ガイドライン」としている
  - 「指針」に示された項目は、各分野の「安全基準等」に盛り込まれている（規定する必要がない場合を除く）
- 「指針」の位置づけの検討に際して、行動計画見直しの基本的スタンス・視点として整理された「重要インフラ事業者等の自主的な取組みが大原則」 及び「実態を把握した上で現実の具体的な経緯に即した課題の検証」を行うという点について留意すべきではないか

【事務局案】
- 論点整理にある「安全基準等」に盛り込む「べき」事項については、盛り込むか「検討するべき」事項（「要検討事項」）と位置づけて、安全基準等に規定する必要があるかを各分野にて検討することとしてはどうか
- その上で、「指針」に記載される事項について、「要検討事項」（「安全基準等」に盛り込むか「検討するべき」事項）と「参考事項」（盛り込むことが「望ましい」事項）に分類してはどうか
- 「要検討事項」には、以下の項目を記載してはどうか
  1）現行の「指針」に示された項目（既に「安全基準等」に盛り込み済みの項目）
  2）現行動計画の取組みに基づく知見・教訓等（例.相互依存性解析の成果）

安全基準等の指針 「Ⅰ4.本指針の位置づけ」より（抜粋）
・重要インフラ分野においてサービス提供継続及び国民の信頼性に応えるとの観点から情報セキュリティ対策を実施する場合、**何らかの対処がなされていることが望ましい項目を列記**し、安全基準等の策定・改定を支援することが本指針の目的である。

事務局案（4-3 安全基準等の整備①）

○記載内容の具体性のレベルとして、現在の「指針」より具体的に記述する必要はあるか

- 現行の「指針」では、「対策項目の具体化は各事業分野又は各事業者毎に検討されることを期待」している
- 現行の「指針」を踏まえ、各分野の「安全基準等」において、「本指針に示された項目を満たすだけでなく、一層高度かつ網羅的な安全基準等」となっている場合もある
- 現行の「指針」の記載内容の具体性のレベルは、現行動計画の策定時点（安全基準等の整備を開始する時点）においては、情報セキュリティ対策の底上げの観点から意義があるものと考えられるが、次の段階を見据えた場合にどのように考えるべきか
  - 「次期情報セキュリティ基本計画に向けた第1次提言」では、「具体的取組みの持続的な推進」や「事故前提社会への対応力強化」が検討されている
  - 指針に示された項目は、各分野の「安全基準等」に盛り込まれている（規定する必要がないものを除く）が、それ以外にも情報セキュリティ対策を行う際に基準又は参考にする文書はないか

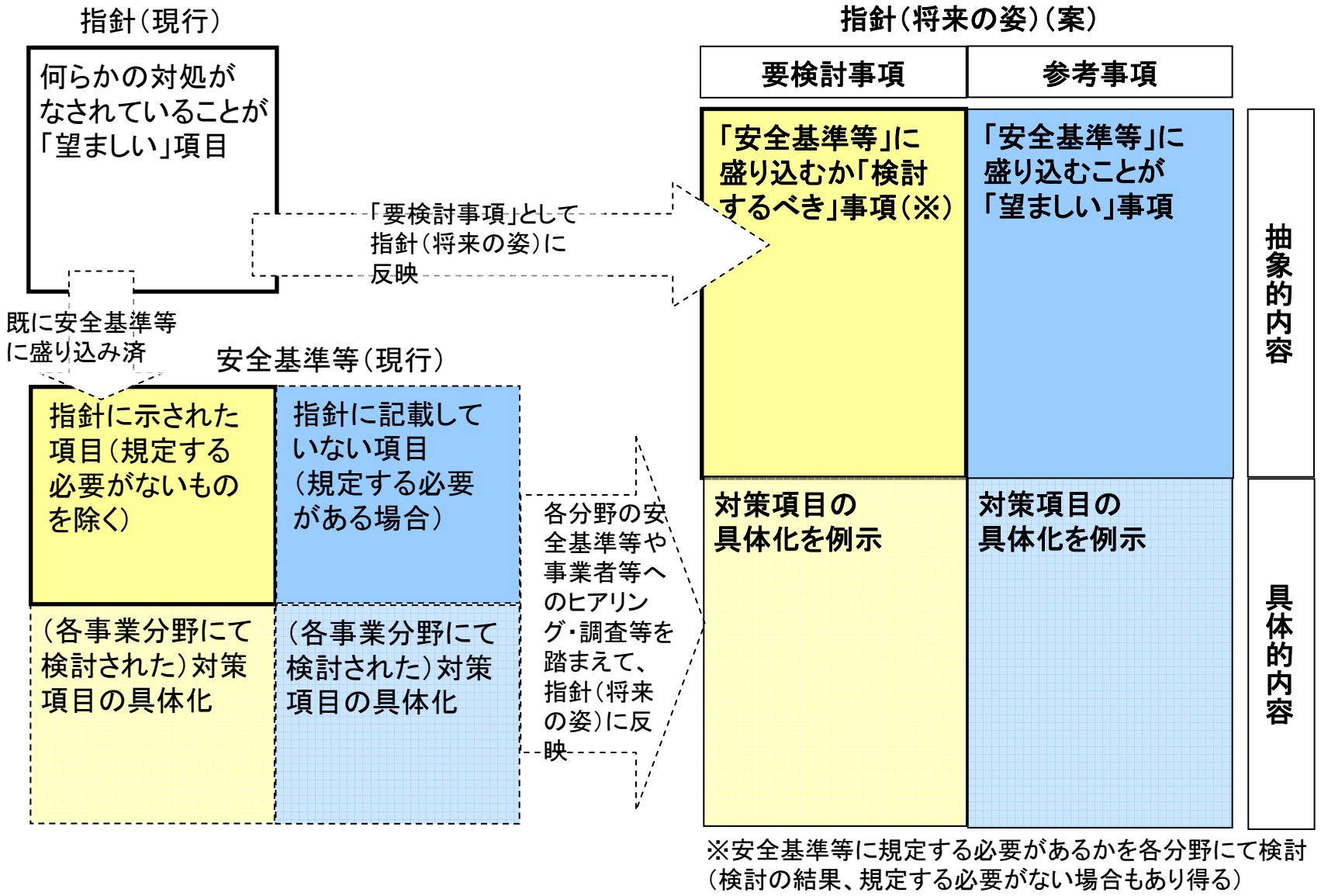
【事務局案】
- 項目レベルの「抽象的内容」に加え、情報セキュリティ対策を例示した「具体的内容」を広く記載してはどうか
- 「具体的内容」は以下の方法にて洗い出してはどうか
  1）現行の「安全基準等」における対策項目の具体化より抽出
  2）各分野・事業者等へのヒアリング・調査等より対策項目の具体化を収集
- 各分野は、「安全基準等」の見直しの中で、関係する「基準又は参考にするものとして策定された文書類」を広く「安全基準等」として位置づけてはどうか

安全基準等の指針 「Ⅰ4.本指針の位置づけ」より（抜粋）
・重要インフラ分野及び事業者によって、それぞれの項目の重要度が異なると考えられることから、本指針では項目を記載するに留めており、**対策項目の具体化は各事業分野又は各事業者毎に検討されることを期待**する。

同 「Ⅰ5.本指針を踏まえた安全基準等策定若しくは見直しへの期待」より（抜粋）
・個々の安全基準等においては、より高度な情報セキュリティ水準の実現を目指し、**本指針に示された項目を満たすだけでなく、一層高度かつ網羅的な安全基準等**となるよう、随時検討がなされることを期待する。

事務局案（4-3 安全基準等の整備①）

指針の位置づけ、記載内容の具体性のレベル（イメージ）



＜参考＞　重要インフラ各分野の安全基準等

分野		安全基準等の名称 【発行主体】 ※2008年2月時点	指針に基づく分類（※1）			
			①	②	③	④
情報通信	電気通信	電気通信事業法、電気通信事業法施行規則、事業用電気通信設備規則等（関連する告示を含む） 情報通信ネットワーク安全・信頼性基準【総務省】 電気通信分野における情報セキュリティ確保に係る安全基準（第1版）【ISeCT】（※2）	○	○	○	
	放送	放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン 【日本放送協会（NHK）、（社）日本民間放送連盟】			○	
金融		金融機関等におけるセキュリティポリシー策定のための手引き【FISC】（※3） 金融機関等コンピュータシステムの安全対策基準・解説書【FISC】 金融機関等におけるコンティンジェンシープラン策定のための手引書【FISC】			○ ○ ○	
航空	航空運送	航空運送事業者における情報セキュリティ確保に係る安全ガイドライン【国土交通省】			○	
	航空管制	航空管制システムにおける情報セキュリティ確保に係る安全ガイドライン【国土交通省】				○
鉄道		鉄道分野における情報セキュリティ確保に係る安全ガイドライン【鉄道事業者等】			○	
電力		電力制御システム等における技術的水準・運用基準に関するガイドライン【電気事業連合会】			○	
ガス		製造・供給に係る制御系システムの情報セキュリティ対策ガイドライン【（社）日本ガス協会】			○	
政府・行政サービス		地方公共団体における情報セキュリティポリシーに関するガイドライン【総務省】			○	
医療		医療情報システムの安全管理に関するガイドライン第2版【厚生労働省】		○		
水道		水道分野における情報セキュリティガイドライン【厚生労働省】		○		
物流		物流分野における情報セキュリティ確保に係る安全ガイドライン【国土交通省】		○		

（※1）①：業法に基づき国が定める「強制基準」
②：業法に準じて国が定める「推奨基準」及び「ガイドライン」
③：業法や国民からの期待に準じて事業者団体等が定める業界横断的な「業界標準」及び「ガイドライン」
④：業法や国民及び契約者等からの期待に応えるべく事業者自らが定める「内規」
（※2）ISeCT：電気通信分野における情報セキュリティ対策協議会、（※3）FISC：（財）金融情報システムセンター

事務局案（4-3 安全基準等の整備②）

②事業者等のPDCAサイクルとの整合性　【重要整理事項】

○「指針」改定のサイクルや時期について、事業者等の実態に即してどう考えるべきか

- 現行動計画における「安全基準等の整備」施策から、以下の課題が発生している
  - 大規模な改定が必要な場合や検討会等を開催する場合は最低6ヵ月間必要
  - 年度の区切りを鑑み、安全基準等の見直し完了は年度末が適当
  - 事業者等が内規を見直しているのと同時に、次の安全基準等の見直しが行われ混乱
- 2007年度は、指針の見直しの結果、改定は行わずに見直しの要点を参考資料として周知した
- これまで独自のサイクルで安全基準等の見直しを推進している分野も存在する

【事務局案】
- 指針の大枠（「要検討事項」のうち「抽象的内容」）の変更は、原則行動計画の見直しの周期に合わせて行ってはどうか
- 上記以外の部分（「参考事項」全て、及び「要検討事項」のうち「具体的内容」）は、「必要に応じて適時に」見直すものとし、追補版の作成等、原則指針改定以外の方法で周知してはどうか
- 既に全ての分野で安全基準等の整備が完了し、安全基準等の位置づけが業法からガイドラインまで様々であることから、安全基準等の見直し及び浸透の進め方は各分野にて主体的に検討することとしてはどうか

現行動計画「3(1) 位置づけ」より（抜粋）
・指針については、**1年ごと、及び必要に応じて適時に、**見直すこととし、「安全基準等」については、情報セキュリティを取り巻く環境の変化に応じ、随時見直しを行う。

安全基準等の指針「Ⅲ(1)本指針の見直し」より（抜粋）
・内閣官房は、**1年ごと、及び必要に応じて適時に、**本指針の見直しを推進する。

事務局案（4-3 安全基準等の整備②）

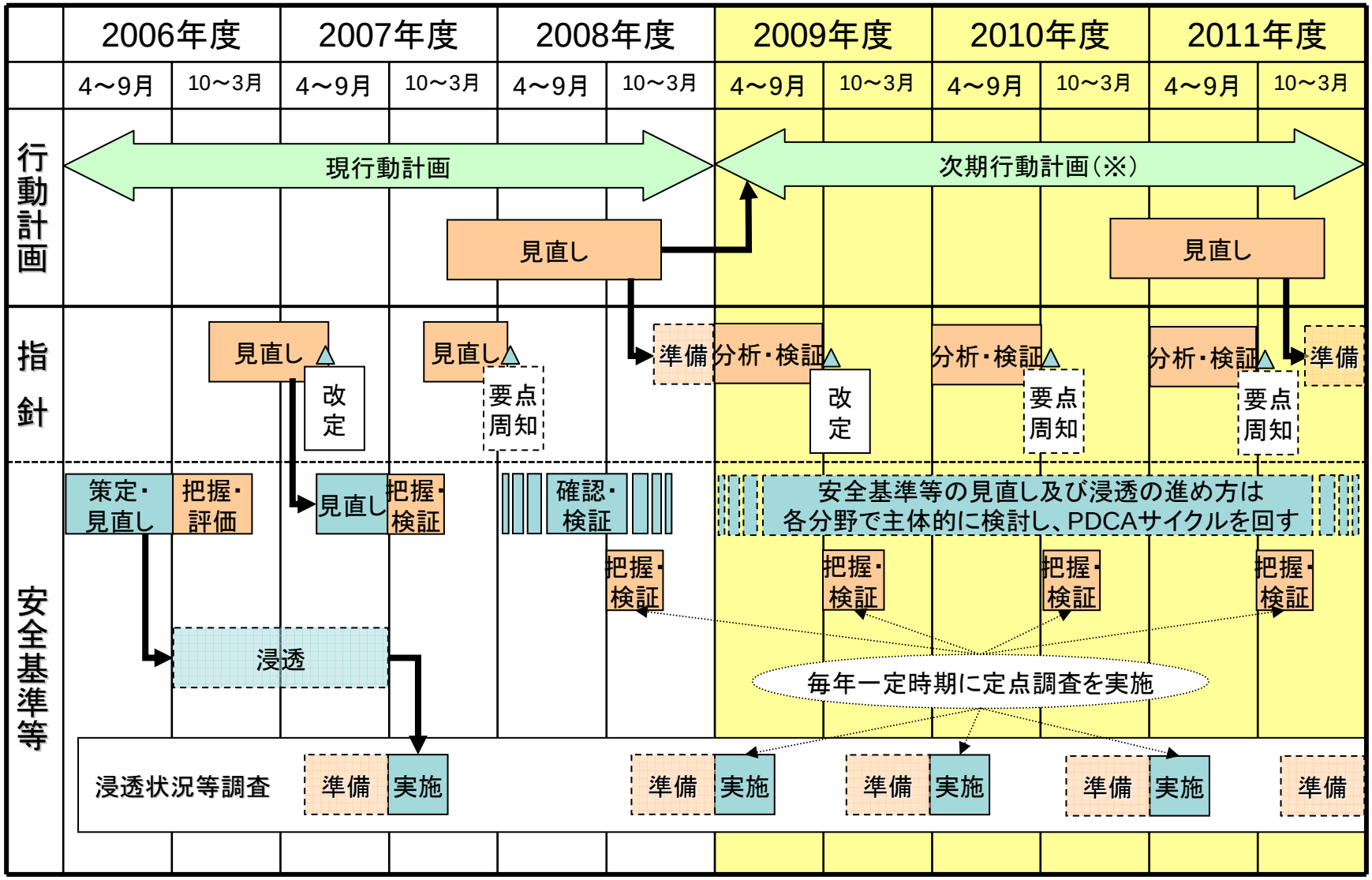
○NISCとして実態を把握するためにはどのような方法が適切か

- 「安全基準等の策定・見直し状況の把握及び検証」にて、以下の各分野の実態を把握した
  - 全ての分野で安全基準等の整備が完了
  - 指針に示された項目は、各分野の安全基準等に盛り込まれている（規定する必要がない場合を除く）ことを確認
  - 指針改定箇所について、各分野の安全基準等が対応していることを確認
- 加えて、2007年度「安全基準等の浸透状況等に関する調査」にて、以下の重要インフラ事業者等の実態を把握した
  - 調査対象範囲における概ね全ての事業者等に安全基準等が認知されている
  - 大半の事業者等が内規を制定済であるとともに、約7割の事業者等で内規見直しが実施・予定されていることが推定
  - 今回初めて自己点検、演習・訓練、内部監査、外部監査の実施状況について調査
- 「安全基準等の浸透状況等に関する調査」にて、以下の留意点・課題を整理している
  - 既存調査を活用することで調査を効率化
  - 調査可能な範囲から取組み、調査対象の拡大は追って検討
  - 既存調査を活用する分野と調査基準日が異なる

【事務局案】
- 各分野はより一層の安全基準等の普及に努めるとともに、NISCは定点調査として、毎年一定時期に各分野の状況把握や事業者等の取組み等の実態把握を行ってはどうか
- 先進的な取組みを行う事業者等についての顕彰を行ってはどうか
- 「安全基準等の浸透状況等に関する調査」は、既存調査等を参考に調査項目・調査主体等について適宜見直しを行ってはどうか

事務局案（4-3 安全基準等の整備②）

「安全基準等の整備」のPDCAサイクル（イメージ）



※次期行動計画の対象期間を3年間と想定して作成

事務局案（4-3 安全基準等の整備③）

③事業継続計画との関係

○「指針」や「安全基準等」に事業継続の観点を補充する必要はないか、盛り込むとすれば、事業継続計画との整合性をどう取るべきか

- 指針では、3つの重点項目にて「IT障害の観点から見た事業継続性確保のための対策」として「事業継続計画との整合性の確保」としての対策が盛り込まれている
  - 記載の仕方にバラツキはあるが、各分野の安全基準等においても盛り込まれている
- 事業継続管理についての国際規格化、ガイドラインの拡充等の動きがある
  - 内閣府防災、経済産業省にて事業継続計画のガイドラインを策定済
  - ITサービス継続性管理の観点で、経済産業省にてガイドラインを策定中

【事務局案】
・昨今の事業継続計画の策定が進みつつある状況を踏まえ、「指針」に事業継続の観点での具体的内容を補充してはどうか
・事業継続計画との整合性をとるため、国際規格化の進展状況等を踏まえつつ、「指針」の見直しを行ってはどうか

安全基準等の指針「Ⅱ3.(4)②　3つの重点項目」より（抜粋）
・ア　**IT障害の観点から見た事業継続性確保のための対策**
（イ）事業継続計画との整合性の確保
事業継続計画が策定される場合は、顕在化する可能性が高いIT障害として様々なケースを想定して事業継続計画に組み入れるとともに、適宜点検し、必要に応じ対策の改善を行うべきである

＜参考＞各分野の安全基準等における具体的な記載内容（例）

（イ）事業継続計画との整合性への配慮（指針）事業継続計画が策定される場合には、顕在化する可能性が高いIT障害として様々なケースを想定して事業継続計画に組み入れるべきである。

分野		指針との対応	対策項目の具体的な記載内容
情報通信	電気通信	指針に示された内容が盛り込まれているだけでなく、具体的な対策と対策チェックシートの提示がなされている。	・サイバー攻撃対策：対応手順等の整備（危険度のレベル設定／レベル毎の対応フロー）、被害拡大防止措置（トラフィックの緊急的制御、回線／設備の一時停止、攻撃停止要請等）、復旧（攻撃元の特定／恒久的措置等、攻撃元情報の管理）、訓練・演習 ・ネットワーク輻そう対策：対応手順等の整備、検知・被害拡大防止措置（輻そう状態の通知／発生箇所の特定、通信規制措置・解除、加入者端末／回線に対する規制・通知、相互接続網に対する制御・通知） ・その他のIT障害（故障、災害等）対策：対応手順書等の整備（メーカ等の連携） ・重要情報漏えい対策：対応手順書等の整備、被害拡大防止措置
	放送	指針に示された内容は盛り込まれている。	
金融		指針に示された内容が盛り込まれているだけでなく、目的、考え方、実施方法等について具体的な事例を踏まえながら解説がなされている。	・運用管理：障害時・災害時対応策（関係者連絡手順の明確化、対応手順の明確化、障害原因の調査・分析） ・データ保護：漏洩防止（暗証番号等の漏洩防止、相手端末確認機能、蓄積データの漏洩防止策、伝送データの漏洩防止策）、破壊・改ざん防止（排他制御機能、アクセス制御機能、不良データ検出機能）、検知策（伝送データの改ざん検知策、ファイル突合機能） ・不正使用防止：アクセス権限確認（本人確認機能、IDの不正使用防止機能、アクセス履歴の管理）、利用範囲の制限（取引制限機能、事故時の取引禁止機能）、不正・偽造防止対策（カードの偽造防止対策、電子的価値の保護機能、不正検知の仕組み、暗号鍵の保護機能、電子メール、ホームページ閲覧等の不正利用防止機能）、外部ネットワークからのアクセス制限（外部ネットワークからの不正侵入防止機能、接続機器の必要最小限化）、検知策（不正アクセスの監視機能、不正な取引の検知機能、異例取引の監視機能）、対応策（不正アクセス発生への対応策、復旧策） ・不正プログラム防止：防御対策、検知対策、被害時対策
航空		（航空運送事業者） 指針に示された内容は盛り込まれている。	
		（航空管制システム） 指針に示された内容は盛り込まれている。	
鉄道		指針に示された内容が盛り込まれているだけでなく、対策項目の具体化がなされている。	・輸送サービス継続性についての検討
電力		指針に示された内容が盛り込まれているだけでなく、対策項目の具体化がなされている。	・災害時の「災害時対応計画」の策定、サイバー攻撃時の「緊急時対応計画」を策定
ガス		指針に示された内容が盛り込まれているだけでなく、想定し得る最悪のケースの具体化がなされている。	・ガス製造設備の制御システム：ソフトウェア不具合、パラメータ設定ミス ・ガス供給設備の遠隔監視・制御システム：ソフトウェア不具合、ミスオペレーション、通信障害、停電
政府・行政サービス		指針に示された内容が盛り込まれているだけでなく、例文と解説による具体化がなされている。	・例：施設の耐災害性対策、施設・情報システムの地理的分散、非常用電源の確保、人手による業務処理や郵送・電話の利用を含む情報システム以外の通信手段の利用、事態発生時の対応体制及び要員計画等
医療		指針に示された内容が盛り込まれているだけでなく、対策項目の具体化がなされている。	・非常時と判断する仕組み・正常復帰時の手順 ・非常時のユーザアカウントや非常時用機能の管理手順の整備 ・医療施設として定められるBCPにおいては、医療情報システムについての計画を含め、全体としての整合性留意
水道		指針に示された内容が盛り込まれているだけでなく、実施内容の具体化がなされている。	・事業継続ガイドライン（内閣府）、事業継続計画策定ガイドライン（経済産業省）の把握と整合性の取れた対策の盛り込み ・水道供給事業者と受水団体間の整合性留意
物流		指針に示された内容は盛り込まれている。	

事務局案（4-3 安全基準等の整備④）

④リスク開示の在り方

○安全基準等において前提とするリスクを開示することについては、リスク管理の観点からどう考えるべきか

- リスクコミュニケーションの観点から、前提とするリスクを開示することにより、サービス提供側のみでなく利用側におけるリスクの対処が容易になるのではないか
  - リスクを開示せずにブラックボックス化したままでは、利用側にとってみれば、サービス提供側がすべてのリスクを負うという誤解が生じる可能性がある
  - インターネット等を活用して、サービスの停止状況、復旧見込みの情報等を周知している事業者等もある
  - 一方、リスクを開示することにより、攻撃者に対し、脆弱な箇所を知らせることになって、脅威が増大する可能性の側面もある
- 「指針」では、「「安全基準等」は（中略）可能な限り公開されることが望ましい」としている
  - 非公開とする代わりに、情報セキュリティの取組みをホームページに掲示している分野もある
  - 情報セキュリティ政策会議において、「安全基準やこれをふまえたアクションプランについて、重要インフラに依存している国民に公表することが必要」という意見もある
- 情報セキュリティマネジメントの有効性の測定の国際標準（ISO/IEC27004：現在策定中）が参考になるという考え方もある

【事務局案】
・リスクコミュニケーションの観点からの分野や重要インフラ事業者等における様々な自主的な取組み（例．情報セキュリティ報告書の作成）を推奨し、NISCは個人への広報活動の一環として、そのような先進的な取組みの状況を集めて周知することとしてはどうか

事務局案（4-4 情報共有体制の強化①）

①情報共有の目的等について

【重要整理事項】

○「IT障害（リスク）発生時の対応」「経験やベストプラクティスの共有」「一般的な状況認識」など目的や段階に応じて使い分けることを考えるべきではないかといった点や、その前提として、共有が望まれる情報、共有の方法、情報の利用者、利用の仕方、タイミングについて整理すべきではないか

- 実施細目に基づく情報連絡・情報提供やCEPTOAR等の枠組みを適切に活用するため、NISCは共有する情報と活用する枠組みについて整理する必要があるのではないか。
- 共有する情報は脅威ごとに整理し、必要に応じて更に細分化を検討することとしてはどうか。
- 情報の共有にリアルタイム性や確実性が求められる場合は、実施細目に基づく情報連絡・情報提供を利用することが適切であり、それ以外の場合は適宜有効な共有方法を選択することが望ましい。
- 実際に共有する情報についてCEPTOAR-Council（仮称）の創設に向けた活動において、検討中である。
- 共有する情報については、各分野ごとに特性があることを踏まえ、各分野ごとに適した整理をすることが望ましいのではないか。

【事務局案】

・情報共有の整理をするにあたっては、想定される脅威と取り扱う情報の観点からマトリックス的に整理して、共有する情報、共有のタイミング及び共有の方法等を整理してはどうか（イメージは次頁参照）。

・取り扱う具体的な情報や利用の方法等は、NISC、CEPTOAR、CEPTOAR-Council（仮称）等の各主体がそれぞれの主体的な取り組みの中で決めていくものではないか。

・NISCは、関係機関の保有する情報ごとに、重要インフラ事業者等にとって有用な情報提供のありかた（タイミング、様式、方法など）を検討してはどうか。

情報共有の整理イメージ

共有情報 ／ 脅威	A.未然防止及び再発防止の観点で有益な情報				B.障害の拡大防止・復旧のため必要となる情報	
	a.各種規程の紹介	b.個別の事例等に関する情報	c.予兆・警報に関する情報 ア 緊急対応が不要な場合	c.予兆・警報に関する情報 イ.緊急な対応が必要な場合	a.事業者等→所管省庁→NISC	b. NISC→所管省庁→CEPTOAR→事業者等
1. サイバー攻撃 ①サービスの対象となるシステムへの直接的な攻撃 ②サービスが直接のターゲットではないが、重要インフラ事業者等が被害を受ける攻撃 ③インターネットの基幹システム（IX、ルートDNS等）への攻撃	指針の改定 指針見直し文書の公表 安全基準等の見直し状況 国際標準の策定 各種ガイドラインの策定	重要インフラ事業者等の分析報告の公表、プレゼンテーション等 業界レポートの公表、プレゼン等 ベストプラクティスの公表、プレゼンテーション等 関係機関等のレポートの公表	関係機関等から提供される情報 ・ゼロデイ攻撃の情報、DoS、DDoS攻撃予告 ・異常なトラフィック発生 ・注意喚起　等		・障害の状況 ・暫定措置 ・障害の発生原因 ・障害に対する対策 ・復旧見込み ・電気通信、電力、水道（サービスの停止等により他分野の重要システムに影響が波及し得る分野）の各サービスの停止・復旧に関する情報	・障害の状況 ・暫定措置 ・障害の発生原因 ・障害に対する対策 ・復旧見込み ・電気通信、電力、水道の各サービスの停止・復旧に関する情報
2. 非意図的要因 ①プログラムミス、システムの不具合や操作ミス等 ②制度改正等大規模な変化を伴う社会的問題	指針の改定 指針見直し文書の公表 安全基準等の見直し状況 相互依存性解析の報告書の公表 国際標準の策定 各種ガイドラインの策定 制度変更等の紹介	重要インフラ事業者等の分析報告の公表、プレゼンテーション等 ベストプラクティスの公表、プレゼンテーション等 関係機関等のレポートの公表	・基幹システム、ソフトウェアの不具合等に関する情報 ・修正プログラムのインストール時に発生する不具合等に関する情報（例：自動インストールされる場合等） 制度変更等に関する事前（直前）警告等			
3. 災害						
情報共有のタイミング	（ア）平時（要警戒時・障害発生時以外のタイミング） → リアルタイム性は不要			（イ）要警戒時・障害発生時 → リアルタイム性が必要（実施細目に基づく取扱い）		
情報共有の方法	ニュースレターで紹介 重要インフラ向けWeb等で共有	各セプター、セプターカウンシルで共有を期待 ニュースレターで紹介	ニュースレターで紹介	実施細目に基づく情報提供	実施細目に基づく情報連絡（※緊急事態等における別の連絡体制や手続きがある場合を除く）	実施細目に基づく情報提供（※緊急事態等における別の連絡体制や手続きがある場合を除く）

事務局案（4-4 情報共有体制の強化②）

②NISCの役割について　【重要整理事項】

○分析機能や「関係機関」との結節点としての機能など、明確化すべきNISCの役割は何か

- 2007年度の「CEPTOAR-Council検討の場」及び本年度に設置した「CEPTOAR-Council創設準備会」の事務局をNISCが務めている。
- 「2007年度の評価」や「行動計画見直しにあたっての論点整理」を見ると、情報共有体制の有効活用が課題と位置付けられている。
- その一方で関係機関との連携においても、関係機関の様々な活動状況を踏まえながら、連携の方策を検討する必要がある。

【事務局案】

・NISCはCEPTOAR−Council（仮称）の立ち上げに向けて、当面は事務局の役割を担うとともに、その活動の強化のために各CEPTOAR間の連携強化を促進することとし、そのために有効な環境整備に取り組んではどうか。

・NISCは、関係機関の活動や保有する情報を把握・整理するとともに関係機関等の有する分析機能の活用を検討してはどうか。

・NISCは、重要インフラ事業者等の情報セキュリティ向上のために有用な活動を行う機関を関係機関として適宜追加してはどうか。

・NISCは、定常的な情報発信を行う中で、分野横断的な観点での情報のニーズとシーズの把握を行い、情報提供に適宜フィードバックすることとしてはどうか。

・事例や経験の共有の強化のために、NISCはこれまで実施してきた相互依存性解析で得た観点から事例の分析を行うこととしてはどうか。

事務局案（4-4 情報共有体制の強化③）

③情報共有の障害除去

【重要整理事項】

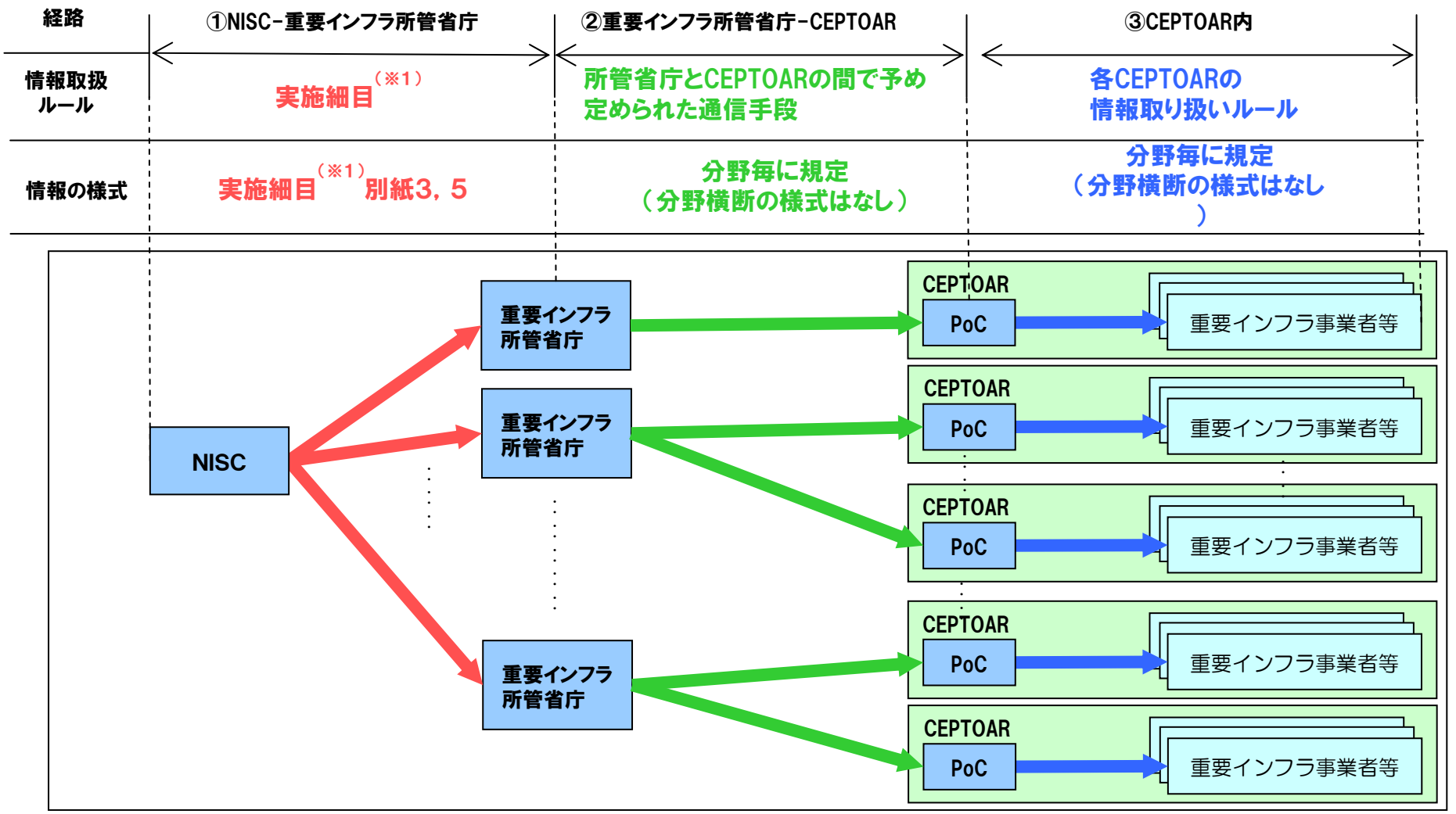
○重要インフラにおける情報共有の障害となりうる事象は何か、それを除去するために有効な方策は何かといった点や、守秘義務や免責等の法律的課題について現実の情報の流れに照らし、現在の「実施細目」等の仕組みにおいて見直すべき部分はあるか

- 情報共有の妨げの要因としては、「事業者等～CEPTOAR～所管省庁～NISC」間で共有する情報、共有が望まれる情報、共有可能な情報や共有の必要性について明確になっていないことが原因ではないか。
- これまでの分野横断的演習やCEPTOAR訓練等の活動を通して、現行の情報共有体制は、経路が3段階から構成され、それぞれの経路間のルールの整合が必要である等様々な課題が挙げられている。
- 現行の情報共有体制は政府間の情報取り扱いを定める「実施細目」(※1)から起因する課題が多い。
- 情報共有体制の見直しを考える場合、政府間のルールを定めた「実施細目」に留まらず、情報共有体制の全体的なルールの整合を見直した後、実施細目も含めて細部の見直しに着手すべき。

【事務局案】
・共有する情報については、サービスの定義や対象とする脅威の検討を踏まえた上で、整理することとしてはどうか。
・体制としては行動計画別紙3－1に示す現行を踏襲し、課題となっている「実施細目」を含めた情報共有体制を構成する各経路間の運用解釈に係る認識を整合させるために、運用方法の明確化をしてはどうか。
・但し、CEPTOAR-Council（仮称）については今年度末に設置が予定されているものであることから、別紙3－1上のCEPTOAR-Council（仮称）に係る記載については、CEPTOAR-Council（仮称）創設準備会の検討状況を踏まえつつ別途整理してはどうか。
・CEPTOARとの情報取扱いルールの整合の際には、CEPTOAR-Council（仮称）で議論してはどうか。

（※1）「重要インフラの情報セキュリティ対策に係る行動計画」の情報連絡・情報提供に関する実際細目

【参考】情報共有体制における各々の経路と情報共有体制の現状



（※1）「重要インフラの情報セキュリティ対策に係る行動計画」の情報連絡・情報提供に関する実際細目

事務局案（4-4 情報共有体制の強化④）

④CEPTOARについて

○各重要インフラ分野における主体的取組みの下で、重要インフラにおける情報共有を進めるという観点から、CEPTOARがより有効的かつ効果的に機能するための工夫は考えられないか

- 2007年度末に新規3分野においてCEPTOARが整備されたことにより、重要インフラ全分野においてCEPTOARが整備されたが、整備されたばかりのCEPTOARについては活動による蓄積が少ないことから機能の確立、充実を図ることに留意する必要がある。
- 複数のCEPTOARにおいては、先進的な活動として対政府の窓口機能だけでなく、CEPTOAR独自の機能として分析機能等を保有している。（ただし、分析の内容は分野によって様々である。）
- CEPTOARについては、引き続き政府からの情報の共有を推進するとともに、今後は、CEPTOARにおける情報の収集、把握・分析、内部での共有、他CEPTOARやCEPTOAR-Council（仮称）等への発信などといった機能の展開が期待される。

【事務局案】
・NISCは、CEPTOARが有効に機能するために共有する情報や利用の方法等の整理の促進、先進的なCEPTOARの活動の紹介等を行い、各CEPTOARの機能充実を支援することとしてはどうか。
・NISCは、CEPTOARを効果的に支援する観点から各CEPTOARの活動状況を適切に把握していくこととしてはどうか。
・NISCは、国民への説明責任を果たしていく観点から、把握している各CEPTOARの活動状況をCEPTOARに支障のない範囲で整理して国民に対して説明していくこととしてはどうか。
・NISCは情報提供を活性化するとともに、CEPTOARの情報共有体制の維持・向上のために情報疎通機能の確認等の機会を提供してはどうか。

(2) 情報共有・分析機能（CEPTOAR）
IT障害の未然防止、発生時の被害拡大防止・迅速な復旧及び再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係重要インフラ事業者等間で共有することにより、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資するため、各重要インフラ分野内に「情報共有・分析機能」（CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response）の整備を進める。

事務局案（4-4 情報共有体制の強化⑤）

⑤その他

○情報共有体制の充実強化のためには、行動計画上の「関係機関」や、「基幹システム」との連携についても検討すべきではないか、その他連携を検討すべき相手はないかといった点や、IT障害に至らない、いわゆる「ヒヤリハット」についても共有できるような体制が必要ではないか

- IT障害の事例の共有と共に、情報セキュリティ上の問題が発生しながら、適切な対応が行われた事例などIT障害に至らなかった事例に関する情報の共有についても重要である。
- IT障害の中でも、情報連絡の対象となるのは、法令等で報告が義務づけられているものや重要インフラ事業者等が特異重大なものと判断したものに限られる。
- 実際、2007年度の指針見直しの中で、過去事例の知見や教訓を踏まえたことにより、未然防止や被害軽減が実現できた事例もあることが確認されている。
- 但し、情報共有を行う体制については、新たに構築することを検討する前に、現時点で構築されている体制の活用をする方が効率的である。

【事務局案】
・IT障害に至らない事例や現行情報連絡の対象とならないIT障害の事例の共有についてはNISCによる関係機関等との情報共有を含めた支援のもとでCEPTOAR及びCEPTOAR-Council（仮称）等の民主体の活動に期待することとしてはどうか。また、官民の情報提供連絡体制として、情報共有を図ることについても検討してはどうか。
・事例や経験の共有の強化のために、NISCはこれまで実施してきた相互依存性解析で得た観点から事例の分析を行うこととしてはどうか。

イ 重要インフラ事業者等からの情報連絡
① 情報連絡の対象となるIT障害（別紙3－2～4参照）
情報連絡の対象となるIT障害は、次に掲げる場合であって、法令等で報告が義務づけられている事故、障害、業務遅延等のほか、特異重大なものとして重要インフラ事業者等が連絡を要すると判断したものを含むものとする。

事務局案（4-5 相互依存性解析・分野横断的演習①）

①相互依存性解析の継続について　【重要整理事項】

○次期行動計画においても、引き続き相互依存性解析を行う意義、目的はあるか、引き続き行うとした場合、実施体制や方法について見直す必要はないか。また、例えば対象とするシステムを拡げたり、事業復旧計画レベルでの相互依存性を検証するなど、新たな検討項目を追加する必要はないか

- 各重要インフラ分野におけるIT利用が進展するにつれ、重要インフラ分野相互の依存関係が増大しつつある中、重要インフラの情報セキュリティ対策を向上させていくためには、引き続き分野横断的な状況の把握・解析が不可欠ではないか
- 解析結果は重要インフラ事業者等の「安全基準等」策定・見直しに活かされつつあるが、事業継続計画の策定や重要インフラ所管省庁の政策・検査などへの反映も期待されるのではないか
- これまでの取り組みを通じて、関係者間の人的ネットワークが形成・強化されているのではないか
- 解析の目的を達するためには、これまでの方法で十分であったと言えるのか
- 専門家による研究的な取り組みとしてはどうか
- 対象とするシステムを拡大するかどうかにあたっては、まず対象とするサービスをどう考えるかが前提となるが、それにはサービスの範囲を利用者の視点でとらえる必要があるのではないか

【事務局案】
- 相互依存性については、関係者間で一定の共通認識が得られるなど成果があがっており、より一層の活用ができるよう、引き続き行うこととしてはどうか
- 研究者等との連携をより深めつつも、基本的な枠組みは現状のNISC、重要インフラ所管省庁、重要インフラ事業者等という取り組みとしてはどうか
- 具体的方法としては、特定テーマ（関係性）に基づき分野間に焦点を当て、限られた関係者間で情報管理に、より配慮した形で調査を行うこととしてはどうか。又、そのアウトプットの公開については、関係者間で可能な範囲を設定し情報共有することとしてはどうか
- 引き続き事業復旧計画に資する視点を重点にし、対象とするシステムには、利用者がサービスを受ける過程で必要な一連の手続きに関するシステムも含めることとしてはどうか

事務局案（4-5 相互依存性解析・分野横断的演習②）

②分野横断的演習の継続について　【重要整理事項】

○次期行動計画においても、引き続き分野横断的演習を行う意義や目的はあるかといった点や、引き続き行うとした場合、例えば既に行った演習テーマの掘り下げや、演習規模の拡大など、向かうべき方向性についてどう考えるべきか、実施体制や方法について見直す必要はないか

- 2006年度の机上演習、2007年度のより実態に近い形での機能演習といった分野横断的演習を通じてIT障害発生時における官民の連絡・連携体制と対応能力は着実に向上しているのではないか
- 次期行動計画においても，各施策をより実効性のあるものとするには、分野横断的な演習の実施による検証、見直しが必要ではないか
- 事業者にとってメリットのある演習とはどういうものか

【事務局案】
・分野横断的演習は段階的に実施していることもあり、引き続き「重要インフラ事業者等の事業継続」に焦点をおいて、分野横断的な課題の抽出を目的として実施するのが望ましいのではないか。
・より成果をあげるために、訓練的な要素を取り入れた演習や、仮説に基づいた演習を実施してはどうか。
・参加分野を絞って掘り下げた演習を行ってはどうか。
・必要に応じて関係機関、ITベンダー等の参加による演習規模の拡大を行ってはどうか。

事務局案（4-5 相互依存性解析・分野横断的演習③）

③事案対処の観点からの課題検証について

○分野横断的演習において「事案対処」の観点からの課題について検証する場合、その方法として如何なる方法が適当か。また、その際には「事案対処省庁」との連携のあり方や課題についての具体的検討が必要ではないか

- 分野横断的演習は、「IT障害からの早期復旧、事業継続（重要インフラ事業者等のサービスの維持及びIT障害発生時の迅速な復旧等の確保）」等の観点に焦点をおいて、分野間の相互依存関係の検証や情報提供・情報連絡といった分野横断的課題の抽出を目的として、段階的に実施してきている
- 「事案対処省庁」との連携のあり方や課題についての具体的な検討を行う際には、「IT障害からの早期復旧、事業継続」等の観点からどのような協力が可能なのかを整理する必要があるのではないか。

【事務局案】

・意図的要因によるIT障害発生時には、「事案対処」の観点からの対応もあるが、「事案対処」は基本的には決められた法的枠組み等に基づいて行われるものであり、課題抽出を目的とした本演習での検証にはなじみにくい面があるのではないか

・「事案対処省庁」との連携のあり方や課題について検討するに当たっては、分野横断的演習の目的である「IT障害からの早期復旧、事業継続」等の観点から「事案対処省庁」から提供される知見や取り組みの内容、有効性等の検討を行い、目的に応じた具体的な連携の検討や連携体制の構築を関係者間で行うべきではないか

・NISCや分野横断的演習の検討の場を通じて、「事案対処」の観点からの知見提供による関係者間の相互理解や信頼関係の増進を図るといったことから始めてはどうか

事務局案（4-5 相互依存性解析・分野横断的演習④）

④その他

○解析や演習を行うに当たっては、事業者の意思決定プロセスも踏まえた検証とする必要があるのではないか

○他に実施される関連演習との連携や、国際的連携の可能性について

- 事業者の意思決定プロセスなど現実的な要素も取り入れ，事業者にとって有意義な演習にすべきではないか
- ITの普及により，情報に関する距離は国内はもとより国際間においても急速に縮まっており、IT障害による被害の規模、波及範囲も格段に大きくなってきているのではないか

【事務局案】
- 事業者の意思決定プロセスを踏まえるなど、より現実に近づけた形での演習を志向してはどうか
- 解析や演習の更なる推進のためには、国内外の関連した取り組みとの情報交換や情報共有、共同取り組みといった連携強化に一層努めてはどうか